SERVICE SCHEDULE

PULSANT MANAGED FIREWALL

This is a Service Schedule as defined in the Conditions. Where the Services set out in this Service Schedule form part of the Services to be supplied under a Contract (as defined in the Conditions), this Service Schedule forms part of the Contract.

In this Service Schedule, references to Clauses are to Clauses of the Conditions, and references to paragraphs are to the paragraphs of (i) this Service Schedule or (ii) whichever other document is specifically referred to.

1 Additional Definitions

In this Service Schedule the following words and expressions shall have the following meanings:

1.1 "**Firewall**" — a physical or virtual device used to enforce data security and access policy at the perimeter between two or more networks.

1.2 "**High-Availability Pair**" — A pair of identical Firewalls configured to work together such that with the failure of one device the second device automatically continues to provide the Service.

1.3 "**Next Business Day**", "**NBD**" — Next business day support for call-out hardware replacement. In the event of a hardware failure it will be replaced the following business day from when it was reported to the vendor, noting that NBD support is only available weekdays during regular office hours and as such a weekend failure may result in hardware replacement the following Tuesday.

2 Pulsant Managed Firewall– Service Scope and Description

2.1 Pulsant Managed Firewall Service provides the Customer with a managed physical or virtual Firewall device that is dedicated to the Customer's use.

2.2 The Customer confirms that it has considered and accepts full responsibility for all scenarios relating to any failure conditions and functionality of each related or dependent service where those services are not provided by the Supplier.

2.3 Pulsant Managed Firewall Services are provided to the Customer for so long as the Contract remains in force in accordance with the terms of the Contract and the Supplier's acceptable use, security, and access policies and procedures.

2.4 Pulsant Managed Firewall Services are subject to payment by the Customer of the Supplier's Charges for installation and support services, as set out in the Order Form or as subsequently agreed between the parties from time to time.

2.5 Any supplied hardware remains the property of the Supplier and is made available for the Customer's use for so long as the Contract remains in force.

2.6 Where diagnostic services are required to identify any issue or potential issue, the Supplier will only provide end-to-end diagnostics if the connectivity, hardware and software is entirely managed by the Supplier. If any elements are shown not to be managed by the Supplier, then any end-to-end diagnostic services will be stopped.

2.7 Managed Firewalls are supplied as single devices or as a High-Availability Pair of devices configured with resiliency features that act as one logical Firewall. Where a High-Availability Pair of Firewalls is provided this will be detailed on the Order Form. A High-Availability Pair cannot subsequently be split into two separate individual managed devices.

2.8 The Supplier will provide the Customer with the following:

2.8.1 A Firewall as either a physical or virtual device, or two devices configured as a High-Availability Pair, installed in a Supplier data centre or on the Customer's designated premises, as specified on the Order Form.

2.8.2 Initial configuration of the Firewall, including::

2.8.2.1 Physical or virtual network interfaces.

2.8.2.2 Up to five (5) logical VLAN interfaces.

2.8.2.3 Inbound access control lists (ACL) specifying destination IP address and/or protocol and/or port.

2.8.2.4 Outbound access control lists (ACL) specifying destination protocol and/or port.

2.8.2.5 Up to ten (10) outbound access control lists (ACL) specifying destination IP address.

2.8.2.6 Routing configuration for required interface routes plus up to five (5) additional routes.

2.8.2.7 One (1) network/port address translation (NAT) rule per configured destination IP address, plus up to five (5) additional rules.

2.8.2.8 Up to five (5) site-to-site virtual private network (VPN) connections.

2.8.2.9 Global Protocol Inspection Service Policies.

2.8.2.10 Remote Access virtual private network (VPN) with a single VPN endpoint.

2.8.2.11 High Availability in Active/Passive mode, if specified on the Order Form.

2.8.2.12 Multi-factor authentication using Pulsant Managed MFA service, if specified on the Order Form.

2.8.2.13 Any configuration in addition to that listed in this paragraph 2.8.2 may be performed on request, subject to additional charge.

2.8.3 A valid SSL certificate, at additional cost, if required by the deployed functionality. The Customer accepts that there may be a delay in supplying this as certificate identity validation is outside the control of the Supplier and may require Customer action.

2.8.4 Firmware and software upgrades of the Firewall or its management components, applied as recommended by the firewall vendor for the lifetime of the Service.

2.8.5 Continuous monitoring of Service availability.

2.8.6 Diagnosis of faults within the Firewall.

2.8.7 Diagnosis of connectivity faults across the Supplier's managed infrastructure only; diagnosis will halt when it is determined that an issue involves infrastructure not managed by the Supplier.

2.8.8 Live performance analysis of Firewall throughput, connection throughput, and VPN throughput.

2.9 The Supplier will not provide education around the use of the device or management interfaces.

3 Customer Responsibilities

3.1 Where the Firewall is hosted on the Customer's own or nominated third-party premises, the Customer will:

3.1.1 Provide redundant power provision adequate for powering the equipment at peak consumption.

3.1.2 Provide air conditioning adequate for cooling the equipment at sustained peak load, including appropriate humidity management.

3.1.3 Maintain physical security of the equipment.

3.1.4 Provide and maintain permanent out-of-band management connectivity to the equipment from the Supplier's remote management system.

3.2 In the event that the Supplier considers, in its reasonable opinion, that the Customer fails to meet any of its responsibilities in paragraph 3.1, then the Service Levels in paragraph 4.4 shall not apply.

4 Service Levels

4.1 The supplier will use its reasonable endeavours to deliver the following Response Times, Fix Times and Availability as classified in the tables below.

4.2 Incident Response Times

Event Priority	Definition	Service Hours	Response Time
P1	• Total loss of production service; or • A significant revenue, operational, or safety impact on the entire company; or • Service degraded, affecting the entire company	24/7/365	Within 15 minutes
P2	• Partial loss of service affecting the company; or • Service degraded, affecting multiple departments or a single site; or • There is the potential of significant revenue, operational, or safety impact to the company if not resolved quickly	24/7/365	Within 30 minutes
P3	• Service degraded, affecting non-production services; or • Loss of service affecting a single user	Business Hours	Within 1 Hour
P4	• Degraded service affecting a single user	Business Hours	Within 2 Hours
P5	• Request for information	Business Hours	Within 4 Hours

4.3 Service Availability – Hosted Service

Measure	Description	Value	Fee Credits
Service Hours	The hours during which the service and SLA is provided	24/7/365	
Availability: Single Device	% of the service hours during which service availability is guaranteed (excluding Planned Maintenance)	99.84%	Pro rata proportion of the Monthly Charges for any Non-Availability Period
Availability: High-Availability Pair	% of the service hours during which service availability is guaranteed (excluding Planned Maintenance)	100%	Pro rata proportion of the Monthly Charges for any Non-Availability Period
Hardware Fix	The period of time after diagnostics confirm hardware replacement is required to action the hardware replacement.	5 hours	Pro rata proportion of the Monthly Charges for any Non-Availability Period

4.4 Service Availability – On Premise Service

Measure	Description	Target Availability	Fee Credits
Service Hours	The hours during which the service and SLA is provided	24/7/365	
Availability: Single Device	% of the service hours during which service availability is guaranteed (excluding Planned Maintenance)	99.84%	Pro rata proportion of the Monthly Charges for any Non-Availability Period
Availability: High-Availability Pair	% of the service hours during which service availability is guaranteed (excluding Planned Maintenance)	100%	Pro rata proportion of the Monthly Charges for any Non-Availability Period
Hardware Fix	The period of time after diagnostics confirm hardware replacement is required to action the hardware replacement.	5 hours or Next Business Day (as specified on the Order Form)	Pro rata proportion of the Monthly Charges for any Non-Availability Period

4.5 Fee Credits

4.5.1 Any Fee Credits which fall due pursuant to paragraphs 4.3 and 4.4 above are payable subject to and in accordance with the terms contained in the Conditions.

4.5.2 A pro rata proportion shall be calculated according to the number of complete minutes in the relevant calendar month and the number of complete minutes of Non-Availability in that calendar month.

4.5.3 “Monthly Charge” means the recurring Charges for the relevant Services for the relevant calendar month, net of VAT.

4.5.4 "Availability" means the percentage of the Service hours during which Service availability is guaranteed, not including Planned Maintenance.

4.5.5 “Non-Availability” means a period of time during which the relevant Services is unavailable in breach of the Target Availability Service Level set out in paragraphs 4.3 and 4.4 above.